Co nového v přírodních vědách

Tajemství přirozných čísel *aneb* Proč hledáme velká prvočísla

EDUARD FUCHS

Občas se lze v tisku, který se alespoň v nějaké míře věnuje vědě, dočíst, že bylo nalezeno další prvočíslo. Předpokládám, že „normálního" člověka, který si této zprávy povšimne, nutně napadnou minimálně dvě následující otázky: *A co je na tom pozoruhodného? Vždyť v době počítačů to snad nemůže být žádný problém.* A druhá otázka: *A k čemu je to vlastně dobré?*

Pokusme se alespoň částečně ukázat, že tyto výsledky vůbec nejsou samozřejmé a že – byť se to na první pohled možná nezdá – jsou i z praktického hlediska mimořádně důležité.

Několik slov úvodem

Naši předchůdci před mnoha tisíciletími začali vytvářet první abstraktní pojmy. Záhy jistě vyvstala potřeba jistého počítání, ať již šlo o určení počtu ulovených mamutů nebo o záznamy velikosti majetku při prvních směnných obchodech. Z těchto primitivních pokusů, které nám dokládají nálezy tzv. *vrubovek*, se postupně vyvinul pojem *přirozeného čísla*, což jsou čísla 1, 2, 3, ... jimiž určujeme počty předmětů.

Tento pojem je natolik jednoduchý a názorný, že s jeho pochopením nemají potíže ani nejmenší děti a zvládají ho bezproblémově i lidé, kteří o sobě prohlašují, že matematika je nikdy nebavila a k ničemu ji nepotřebují.

Věda se v průběhu staletí rozvinula natolik, že vhled do jejích jednotlivých disciplín je natolik obtížný, že přesahuje možnosti jednotlivce. Kde jsou ony „idylické" doby, kdy ještě v 18. století neexistovali matematikové nebo fyzikové či chemici, ale „přírodovědci", kteří tvořivě pracovali ve všech uvedených oborech (a často nejen v nich). Dnes na této planetě téměř jistě neexistuje člověk, který by mohl oprávněně tvrdit, že rozumí všem disciplínám, které tvoří současnou fyziku či matematiku; a místo matematiky nebo fyziky bychom samozřejmě mohli uvést kteroukoliv další moderní vědu. Mimořádně obtížné je vysvětlit problémy moderní vědy i erudovanému odborníkovi z jiného oboru, natož pak laikovi.

Magické čtverce a dokonalá čísla

Matematika samotná patří k nejstarším vědám, její dějiny počítáme na tisíciletí. Některá její moderní odvětví zná jen několik málo specialistů. Je proto překvapivé, že řada obtížných a dodnes nevyřešených problémů se týká i těch nejelementárnějších pojmů – přirozených čísel. Ukažme si alespoň některé z nich.

Je zajímavé sledovat, jak se různost jednotlivých kultur projevovala i v tom, jaké vlastnosti byly přisuzovány číslům a jak se s nimi nakládalo. Pro ilustraci si vyberme dva typické příklady ze starověku: Řecko a Čínu.

Ke zrodu matematiky jako vědy v moderním slova smyslu došlo v antickém Řecku v 6.-4. stol. př. Kr. Rozhodující roli v tomto procesu sehrála tzv. pythagorejská škola. Je všeobecně známo, jaký význam číslům (rozuměj přirozeným číslům) pythagorejci přikládali. V jejich pojetí bylo možno pomocí čísel a jejich vzájemných poměrů popsat nejen celou tehdejší matematiku, ale i lidské vlastnosti, a dokonce celý Vesmír. A tak se jejich obzvláštní pozornosti těšila přirozená čísla s různými speciálními vlastnostmi, jako např. prvočísla, dokonalá čísla, spřátelená čísla apod., o nichž se zanedlouho zmíníme podrobněji. Ačkoliv vzájemným vztahům čísel přikládali mnohdy až magické vlastnosti, nedospěli Řekové nikdy k magickým čtvercům, které naopak zkoumali ve starověké Číně, v níž jinak v rozvoji matematiky nedosáhli úrovně starověkých Řeků.

Jen málo matematických objektů se vykytuje i mimo matematiku tak často jako právě magické čtverce. Píše se o nich v ryze matematických knihách i v literatuře úrovně – velmi mírně řečeno – nevalné. Vyskytují se v seriózních historických knihách i v literatuře s okultní a zcela nevědeckou a obskurní náplní. Na internetových stránkách lze pod příslušným heslem nalézt stovky odkazů, v nichž je, zvláště pro laika, orientace přinejmenším obtížná. A tak není divu, že samotný pojem „magický čtverec" má v různých pramenech různé významy.

Obecně vzato je magickým čtvercem nazýváno jakékoliv čtvercové schéma nejrůznějších objektů, nejčastěji čísel nebo písmen, rozmístěných podle nějakých pravidel. Obvykle je však magickým čtvercem označována čtvercová síť vytvořená z navzájem různých čísel tak, že součet čísel ve všech řádcích a sloupcích (a často též v úhlopříčkách) je stejný.

Nejjednodušším příkladem takového magického čtverce je následující čtverec, v literatuře obvykle nazývaný Saturn:

4	**9**	**2**
3	**5**	**7**
8	**1**	**6**

Obr. 1: Magický čtverec *Saturn*

Objevení tohoto čtverce souvisí s jednou z nejstarších knih lidské civilizace, s tzv. *Knihou proměn* – čínsky *I-Ťing*, jejíž vznik spadá až do počátku třetího tisíciletí před naším letopočtem. Historie magických čtverců je fascinujícím příkladem vývoje lidského poznání, úspěchů i bludů a omylů. Podrobnější popis se však vymyká tématu tohoto článku.

Jak jsme se již zmínili, Řekové se nikdy k pojmu magického čtverce nedopracovali. O vlastnostech čísel však toho zjistili mnohonásobně více než Číňané. Brzy samozřejmě poznali významnou roli tzv. *prvočísel*, což jsou čísla dělitelná jen jedničkou a sebou samým; prvočísla jsou např. čísla 7, 11, 31, nejsou jimi však např. číslo 15 nebo 100. Prvočísla hrají mezi čísly roli jistých stavebních kamenů: každé přirozené číslo lze jediným způsobem (až na pořadí činitelů) rozložit na součin prvočísel.

Řekové brzy zjistili, že všech prvočísel je nekonečně mnoho. Jednoduchý důkaz tohoto faktu ukázal již vynikající starořecký matematik *Eukleidés* ve své knize *Stoicheia* (česky *Základy),* kterou napsal někdy kolem roku 300 př. Kr. Již Řekové ovšem věděli, že i když víme, kolik všech prvočísel je, ani zdaleka to ještě neznamená, že je snadné tato čísla vyhledat. Čtenář si možná ještě ze školních let pamatuje starověký nástroj na vyhledávání prvočísel, tzv. *Eratosthénovo síto*. Tímto postupem lze hledat „malá" prvočísla, prakticky však příliš použitelný není.

Jak jsme již uvedli, Řekové zkoumali přirozená čísla z nejrůznějších hledisek. Uveďme alespoň jeden z možných příkladů.

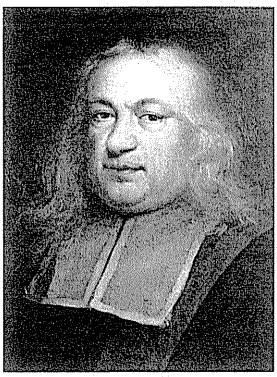
Uvažme nějaké číslo, například 12. To je (kromě sebe samého) dělitelné čísly 1, 2, 3, 4, a 6. Když tyto dělitele sečteme, dostaneme 1+ 2 +3 + 4 + 6 = 16, což je číslo větší než původních 12. Když analogicky sečteme dělitele například čísla 15, obdržíme 1 + 3 + 5 = 9, tedy méně než 15. Ve zcela výjimečných případech se však stane, že součet dělitelů daného čísla je roven číslu samotnému. Tyto případy Řeky fascinovaly a příslušná čísla nazvali *dokonalá*. Sami odhalili jen čtyři taková čísla: 6, 28, 496 a 8 128. (Je např. 1 + 2 + 4 + 7 + 14 = 28.) Dnes známe dokonalých čísel několik desítek, dodnes však nevíme, zda jich je konečně či nekonečně mnoho, a nevíme ani například to, zda existuje nějaké **liché** dokonalé číslo.

Hledání prvočísel

Víme tedy, že prvočísel je nekonečně mnoho. Ačkoliv je matematika zkoumá déle než dva tisíce let, dodnes o nich nevíme řadu věcí. Uveďme například problém tzv. *prvočíselných dvojčat*. Podíl prvočísel mezi přirozenými čísly se postupně snižuje: v první stovce je jich 25, tedy jedna čtvrtina, postupně se však vyskytují stále méně často. Občas se však vyskytnou dvojice „sousedních" prvočísel, jejichž rozdíl je 2: například 11, 13 nebo 29, 31. Právě takovým dvojicím se říká prvočíselná dvojčata. Kolik jich je? To je právě to, co nevíme. Možná konečně, možná nekonečně

mnoho. Žádný počítač nám v tom nepomůže, protože ani ten nejrychlejší počítač nikdy samozřejmě neprojde posloupnost **všech** přirozených čísel.

Jakkoliv se to může zdát podivné, není dodnes ani známa žádná formulka, která by nám umožnila postupně vypočítávat jednotlivá prvočísla. Víme, že jich je nekonečně mnoho, avšak nemáme k dispozici žádný „klíč", který by nám je postupně předváděl. Ačkoliv se nalezení takového vzorce věnovala řada významných matematiků, problém se nepodařilo nikomu vyřešit.



Pierre de Fermat
(1601-1665)

Dodnes nebyl zdolán ani zdánlivě mnohem jednoduší problém: když již neznáme formulku, která by nám postupně umožnila počítat **všechna** prvočísla, spokojili bychom se s formulí, která by nám postupně dávala prvočíselné výsledky, byť ne nutně všechny. O toto se pokusil například již v 17. století geniální francouzský matematik Pierre de Fermat (1601-1665). Není mnoho případů, kdy by se Pierre Fermat mýlil. U prvočísel se mu to však stalo.

V čem spočíval Fermatův omyl? Z řady důvodů dospěl k závěru, že všechna čísla tvaru $VF_n = 2^{2^n} + 1$ jsou prvočísla. (Čtenář si jistě pamatuje smysl uvedených symbolů. Např. 2^n značí součin n dvojek.) Tato čísla rychle rostou; Fermat spočítal prvních pět hodnot

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\ 537,$$

což jsou opravdu prvočísla. V průběhu let se však ukázalo, že další čísla uvedeného tvaru prvočísly nejsou. V roce 1732 dokázal Leonhard Euler (1707-1783), že prvočíslem není číslo $F_5 = 2^{32} + 1 = 4\ 294\ 967\ 297$, v roce 1880 bylo totéž dokázáno pro číslo F_6, a postupně se totéž potvrdilo pro všechna čísla až po číslo F_{23}.

Abychom si uvědomili složitost těchto výsledků, zastavme se na chvíli například u poměrně „malého" čísla F_8. Toto číslo má 39 cifer. Kdybychom zkoumali standardním způsobem, zda je to prvočíslo, museli bychom ho dělit přibližně 10^{36} čísly. I kdybychom měli k dispozici počítač, který by prováděl miliardu dělení za sekundu – a takový počítač v současnosti vůbec neexistuje –, potřebovali bychom přibližně 10^{19} let. Stáří našeho vesmíru je ovšem pouze přibližně 15 miliard let, tj. cca 15 krát 10^9 roků.

Nyní snad aspoň částečně doceníme, jak komplikované muselo být, když se v roce1983 podařilo dokázat, že prvočíslem není číslo F_{23471}. Toto číslo má víc než 10^{7000} cifer. (Tento počet si nesmíme plést s velikostí čísla 10^{7000} . To má „jen" 7001 cifer.)

Dnes převládá přesvědčení, že Fermat se spletl zcela zásadně. S největší pravděpodobností žádné další číslo Fermatem popsaného tvaru, kromě jím popsaných pěti čísel, prvočíslem není. To samozřejmě nesnižuje Fermatův význam. Jen to dokládá, o jak obtížnou problematiku se jedná.

Dnes jsou zkoumána prvočísla tvořená podle nejrůznějších zákonitostí. Ani jedna z metod však není univerzální v tom smyslu, že by nám umožňovala postupný bezproblémový výpočet větších a větších prvočísel. Každá z metod je jen pomůckou, jak lze **snad** nová prvočísla získávat.

Nejvhodnější k tomuto účelu se ukázala být tzv. *Mersennova* prvočísla.

Mersennova prvočísla

Marin Mersenne (1577-1648) byl významným organizátorem pařížského vědeckého života. V jeho bytě se scházely vůdčí osobnosti francouzské vědy první poloviny 17. století, s řadou dalších vědců, včetně například P. Fermata, si dopisoval. Ačkoliv se matematikou zabýval jen okrajově, byla po něm – díky jisté hypotéze, kterou vyslovil – pojmenována prvočísla jistého tvaru.

Marin Mersenne (1577-1648)

Již Eukleidés znal následující skutečnost. Uvažujme čísla M_n tvaru $2^n_n - 1$. Když číslo *n* **není** prvočíslo, pak ani číslo M_n prvočíslem **není.** Pokud číslo *n* prvočíslem **je**, pak M_n prvočíslem **být může**. (Tato prvočísla se dnes právě nazývají Mersennova.) A Řekové skutečně znali prvočísla $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ a $M_{13} = 8191$. V průběhu staletí byla postupně nacházena další prvočísla daného tvaru. Do konce 19. století jich bylo známo 12. Největší z nich, číslo M_{127} , bylo objeveno v roce 1876, mělo 39 cifer a zdálo se, že tímto číslem se matematika dostala na hranice svých možností. Velikost tohoto čísla (čtenář nechť si vzpomene na údaje o Fermatově čísle M_8) přesahovala meze lidských výpočetních možností.

Ve druhé polovině 20. století se však objevily počítače, které kromě jiného umožnily objevovat větší a větší prvočísla. A ukázalo se, že z mnoha důvodů jsou právě Mersennova prvočísla nejvhodnější mezi možnými adepty na testování kandidátů na prvočísla. Do roku 1978 tak bylo známo již 25 Mersennových prvočísel. Největší z nich, M_{21701}, již mělo 6 533 číslic. A vývoj se nezastavil. Brzy se však ukázalo, že náročnost příslušných výpočtů přesahuje možnosti i těch nejvýkonnějších počítačů současnosti. Proto byla zorganizována mezinárodní spolupráce, podobná té, která testuje na tisících počítačů z celého světa, zda některé signály z vesmíru ne-

mohou být signály hvězdných civilizací. Skupinou nadšenců byl zorganizován projekt GIMPS (The Great Internet Mersenne Prime Search), do něhož se zapojily stovky lidí z celého světa, na jejichž počítačích se paralelně provádějí potřebné výpočty. A velikost nalezených prvočísel přesáhla veškerou představivost.

Posledním dosaženým výsledkem je nalezení v pořadí již dvaačtyřicátého Mersennova prvočísla. Dne 18. února 2005 bylo nalezeno prvočíslo $2^{25\,964\,951}-1$, které má 7 816 230 cifer! Jen pro představu: kdybychom chtěli toto číslo vytisknout drobným novinovým písmem, pak by jeho zápis byl dlouhý téměř 19 kilometrů.

Přes nepředstavitelnou velikost tohoto čísla je však nutno si uvědomit, že i těchto Mersennových prvočísel známe jen 42. A nevíme, zda prvočísel tohoto tvaru je nekonečně mnoho nebo zda existuje nějaká hranice, za níž se již nevyskytují.

A proč tato čísla vlastně hledáme?

Snad se nám podařilo aspoň částečně demonstrovat, jak obtížné je získávání velkých prvočísel. Nezodpovězena však zůstává druhá otázka z úvodu: *K čemu je to vlastně dobré*?

Svým způsobem je tato otázka, alespoň pro vědce, nemístná. Problémy řešíme nejen z důvodů ryze „praktických", ale proto, že existují. Stejně tak bychom se mohli ptát, k čemu je dobré lézt na vrcholky velehor, malovat obrazy nebo proč dospělí lidé běhají v dresech po trávníku a snaží se dopravit míč do soupeřovy branky (a navíc jsou za tuto činnost honorováni mnohonásobně více než lidé za hledání prvočísel).

Připusťme však, že taková odpověď nemusí uspokojit tazatele, který nemá přílišné pochopení pro vědu, například ministra financí. I takové tazatele můžeme, naštěstí, snadno uspokojit.

Z řady aplikací, v nichž velká prvočísla hrají zásadní roli, se zmiňme jen o jedné, zato však mimořádně důležité.

Od starověku po současnost byli lidé nuceni najít způsob, jak některé informace utajovat, jak dosáhnout toho, aby u předávaných zpráv zůstával jejich obsah utajen nepovolaným. Řada čtenářů knih A. Dumase nebo J. Verna si jistě vzpomíná na napínavé popisy kódování pomocí šifrovacích tabulek a jiných šifrovacích klíčů.

Nejde však jen o tematiku pro dobrodružné romány a pro příklady nemusíme ani jít do dávné historie. Osudy námořních konvojů v Atlantiku za druhé světové války, životy tisíců lidí a vývoj celého válečného konfliktu, to vše záviselo na tom, zda se podaří prolomit kód, jímž německé velení sdělovalo příkazy svým ponorkám. A takových příkladů bychom mohli uvést celou řadu.

Nejde však jen o vojenství. V současné době oprávněně hovoříme o informační explozi. Množství předávaných informací roste rok od roku

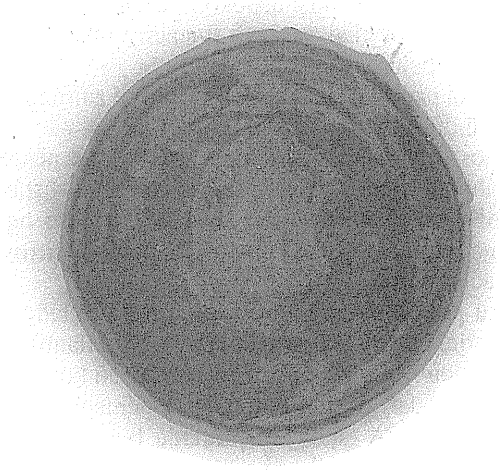
a spolu s tím roste i množství těch zpráv, jejichž zneužití by mohlo způsobit nezměrné problémy. Stačí uvést jen informace o zabezpečení bank, stavech účtů klientů, zpravodajské informace atd.

Historie nás však učí, že každá šifra byla dříve nebo později prolomena, i ty nejdůmyslnější systémy kódování byly časem rozluštěny. Slabým místem všech šifrovacích systémů se vždy ukázalo to, že odesilatel a příjemce zašifrované zprávy si vždy museli vyměnit šifrovací klíč a jakmile se protivník tohoto klíče zmocnil nebo alespoň přišel na jeho strukturu, bylo rozluštění kódu nevyhnutelné. Lze nějak toto omezení obejít?

Ideální by byla taková šifra, že ani prozrazení šifrovacího klíče by nevedlo k jejímu prolomení. Je vůbec možné takovou šifru nalézt?

Odpověď dala moderní matematika: ano takové šifry existují. Šifrovací klíč může být dokonce veřejně známý a nemusí jej opatřovat špióni v riskantních operacích. Tyto šifry jsou založeny na tom, že k jejich rozluštění je nutno obrovská čísla, taková o nichž jsme hovořili, rozložit na součin prvočísel. A jak jsme viděli, i u relativně „malých čísel" by hledání tohoto rozkladu mohlo trvat déle, než je stáří našeho vesmíru. Protivník může vědět, jak lze šifru rozluštit, ale čas na faktické rozluštění prostě nebude mít.

Mohli bychom uvádět i další příklady využití prvočísel. Využívají jich matematické metody, jejichž pomocí byl zkonstruován tomograf, na vlastnostech velkých prvočísel se testují nově vyvíjené počítačové čipy apod. O těchto věcech ovšem Řekové, když objevovali před více než dvěma tisíciletími vlastnosti přirozených čísel, neměli ani tušení. Jak asi odpovídali na otázky svých současníků: *A k čemu je to vaše počítání dobré*?



Otto Piene, Oheň (červená a černá na bílé), 1962